# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/049,812 | 12/27/2001 | Eric J. Sprunk | | 7975 |

20350      7590      09/26/2007
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

| EXAMINER |
|---|
| HOFFMAN, BRANDON S |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/26/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

| | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 10/049,812 | SPRUNK ET AL. |
| | Examiner | Art Unit | |
| | Brandon S. Hoffman | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). ·
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 July 2007*.

2a)☒ This action is **FINAL**.          2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-7 and 10-19* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 10-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References·Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

## DETAILED ACTION

1.    Claims 1-7 and 10-19 are pending in this office action.

2.    Applicant's arguments, filed July 12, 2007, have been fully considered but they are not persuasive.

### Claim Rejections

3.    The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### Claim Rejections - 35 USC § 102

4.    Claims 16-19 rejected under 35 U.S.C. 102(a/e) as being anticipated by Van Oorschot et al. (U.S. Patent No. 5,850,443).

Regarding claim 16, Van Oorschot et al. teaches a method of updating a cryptographic key used for decrypting distributed data, the method comprising:

- Generating a first key for decrypting the distributed data, the first key of a first length (col. 6, lines 25-29);

- Encrypting the first key with a second key, the second key of a second length, wherein the second length is longer than the first length (col. 6, lines 29-31); and

- Distributing the encrypted first key (fig. 1 and col. 6, lines 31-33).

Regarding <u>claim 17</u>, <u>Van Oorschot et al.</u> teaches further comprising distributing

data encrypted with the first key (fig. 2).


Regarding <u>claim 18</u>, <u>Van Oorschot et al.</u> teaches further comprising:

- Generating a third key to replace the first key, the third key of a third length,

  wherein the third length is shorter than the second length (col. 6, lines 46-49);

- Encrypting the third key with the second key (col. 6, lines 43-46); and

- Distributing the encrypted third key (fig. 3).


Regarding <u>claim 19</u>, <u>Van Oorschot et al.</u> teaches further comprising distributing

data encrypted with the third key (fig. 4).


### *Claim Rejections - 35 USC § 103*

5.      <u>Claims 1-7 and 10-15</u> are rejected under 35 U.S.C. 103(a) as being unpatentable

over <u>Menezes et al.</u> (Handbook of Applied Cryptography, 1997, section 13.3.1, pages

551-553) in view of <u>Weiant, Jr. et al.</u> (U.S. Patent No. 6,044,350).


Regarding <u>claim 1</u>, <u>Menezes et al.</u> teaches an asymmetric cryptographic

processing system using a multiple key hierarchy, the asymmetric cryptographic

processing system comprising:

- A first key for performing asymmetric operations at a first rate, wherein each

  operation requires a first cryptographic processing time (page 552, step 3, *data*

*keys*, provide cryptographic operations on user data, tend to be short-term keys);

and

- A second key for performing an asymmetric cryptographic processing operation to update the first key (page 552, step 2, *key-encrypting keys*), wherein the second key is used for cryptographic processing operations for the first key at a second rate that is less often than the first rate (page 552, step 2, *key-encrypting keys*, the key-encrypting keys are used less often than the keys that they encrypt).

Menezes et al. does not specifically teach the second key requires a second cryptographic processing time greater than the first cryptographic processing time.

Weiant, Jr. et al. teaches the second key requires a second cryptographic processing time greater than the first cryptographic processing time (fig. 3).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the second key requiring more processing time than the first key, as taught by Weiant, Jr. et al., with the method/medium of Menezes et al. It would have been obvious for such modifications because longer length keys take more time to process, in order to provide more security, with a tradeoff that the key does not have to be replaced as often.

Regarding <u>claims 2-5</u>, <u>Menezes et al.</u> as modified by <u>Weiant, Jr. et al.</u> teaches

wherein the system is used to cryptographically process and transfer digital

[voice/audio/video] data in a network (see col. 3, lines 32-38 of Weiant, Jr. et al.).

Regarding <u>claim 6</u>, <u>Menezes et al.</u> as modified by <u>Weiant, Jr. et al.</u> teaches

wherein the second key is hard coded into the system at the time of manufacturing the

system (see page 551, section 13.3.1, step 1 of Menezes et al.).

Regarding <u>claim 7</u>, <u>Menezes et al.</u> as modified by <u>Weiant, Jr. et al.</u> teaches

wherein a plurality of digital cryptographic processing systems are coupled by a

telecommunications system, wherein the second key is distributed to two or more of the

asymmetric cryptographic processing systems via the telecommunications system (see

fig. 2 of Weiant, Jr. et al.).

Regarding <u>claim 10</u>, <u>Menezes et al.</u> as modified by <u>Weiant, Jr. et al.</u> teaches a

method for providing secure data transactions in a telecommunications system, wherein

a digital processing device receives information from the telecommunications system

(see fig. 2, ref. num 234 of Weiant, Jr. et al.), wherein the digital processing device uses

a first asymmetrical cryptographically processed key to perform an asymmetric

cryptographic processing operation to decode the information wherein the cryptographic

processing operation is at a first level of complexity requiring a first amount of resources

by the processing device (see page 552, step 3, *data keys* of Menezes et al.), wherein

the cryptographic processing operation is performed at a first rate of cryptographic

processing operations per unit time (see page 552, step 3, *data keys* of Menezes et al.,

provide cryptographic operations on user data, tend to be short-term keys), the method

comprising:

- Transferring a second asymmetrical cryptographically processed key to the

  digital processing device, wherein the second asymmetrical cryptographically

  processed key is used in an asymmetric cryptographic processing operation at a

  second level of complexity requiring a second amount of resources by the

  processing device that is higher than the first amount of resources (see page

  552, step 3, *data keys* of Menezes et al., the data keys are used, perhaps for

  every type of data they encrypt);

- Updating the first asymmetrical cryptographically processed key from time-to-

  time (see page 552, step 3 of Menezes et al.), wherein the updating of the first

  asymmetrical cryptographically processed key occurs at a second rate of

  cryptographic processing operations per unit time that is less than the first rate of

  cryptographic processing operations per unit time (see fig. 3, key B of Weiant, Jr.

  et al.), wherein the updating includes the following substeps:

  o Encoding a substitute first asymmetrical cryptographically processed key

    with a second key, so that the resulting cryptographically processed

    substitute first asymmetrical cryptographically processed key is decodable

    by the second asymmetrical cryptographically processed key (see page

552, paragraph below step 3 of Menezes et al., keys at one layer are used

to protect items at a lower level); and

o Transferring the substitute first asymmetrical cryptographically processed

key to the digital processing device so that the substitute first

asymmetrical cryptographically processed key is used in subsequent

cryptographic processing operations by the digital processing device (see

fig. 2, ref. num 234 of Weiant, Jr. et al.).

Regarding claim 11, Menezes et al. as modified by Weiant, Jr. et al. teaches

further comprising:

- Transferring a third asymmetrical cryptographically processed key to the digital

processing device (see page 551, section 13.3.1, step 1, master key of Menezes

et al.), wherein the third asymmetrical cryptographically processed key is used in

an asymmetric cryptographic processing operation at a third level of complexity

requiring a third amount of resources by the processing device that is higher than

the second amount of resources (see page 551, section 13.3.1, step 1 of

Menezes et al. and fig. 3, key C of Weiant, Jr. et al.);

- Updating the second asymmetrical cryptographically processed key from time-to-

time (see page 552, step 2 of Menezes et al.), wherein the updating of the

second asymmetrical cryptographically processed key occurs at a third rate of

cryptographic processing operations per unit time that is less than the second

rate of cryptographic processing operations per unit time (see fig. 3, key C of

Weiant, Jr. et al.), wherein the updating includes the following substeps:

- o Encoding a substitute second asymmetrical cryptographically processed

  key with a third asymmetrical cryptographically processed key, so that the

  resulting cryptographically processed substitute second asymmetrical

  cryptographically processed key is capable of being cryptographically

  processed by the third asymmetrical cryptographically processed key (see

  page 552, paragraph below step 3 of Menezes et al., keys at one layer are

  used to protect items at a lower level); and

- o Transferring the substitute second asymmetrical cryptographically

  processed key to the digital processing device so that the substitute

  second asymmetrical cryptographically processed key is used in

  subsequent cryptographic processing operations by the digital processing

  device (see fig. 2, ref. num 234 of Weiant, Jr. et al.).


Regarding claims 12-15, the examiner takes Official Notice that the resources

include [processing time/transistor density on an IC/memory capacity/data bandwidth]

because these resources are well-known tradeoffs of resource intensive actions as

cryptography.


### Response to Arguments

6.      Applicant argues:

a.      Van Oorschot et al. does not teach updating a cryptographic key (page 2,

second paragraph through page 3).

b.      Weiant, Jr. et al. does not teach the second key requiring a processing

time greater than the first key or requiring a larger amount of resources to

process than the first key (page 4 through page 5).


Regarding argument (a), examiner disagrees with applicant. The claim language

refers to "generating a first key for decrypting the distributed data, the first key of a first

length; encrypting the first key with a second key, the second key of a second length,

wherein the second length is longer than the first length; and distributing the encrypted

first key". These limitations are shown by the citations of Van Oorschot et al. above.

The step of "updating a cryptographic key" is in the preamble, and therefore carries no

weight.

Regarding argument (b), examiner disagrees with applicant. Figure 3 of Weiant,

Jr. et al. clearly shows that the longer the key, the more time it takes to process the key.

Menezes et al. shows that the key is "updated" by encrypting a short-term key with a

long-term key to create a key-encrypted-key. The key-encrypted-key is an updated

version of the short-term key.


***Conclusion***

7.      The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. U.S. Patent 6,438,666 and U.S. Patent 6,233,341 show that the

longer the key, the more processing time that is required.


8.      **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Brandon S. Hoffman whose telephone number is 571-

272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

9/20/07